BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

W1390

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-008607
(43)Date of publication of application : 10.01.2003

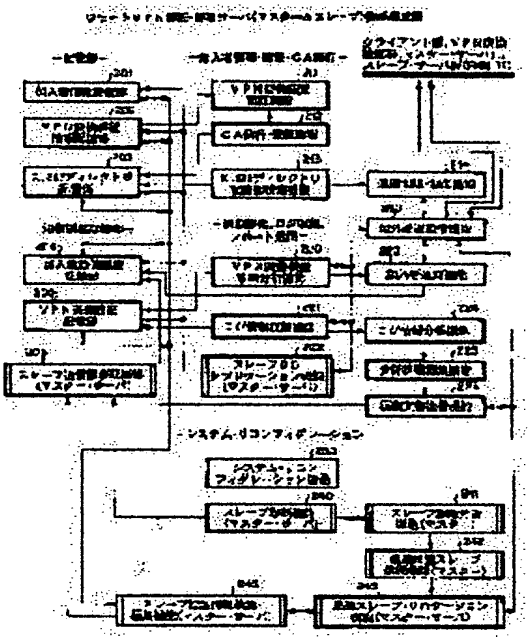
(51)Int.CI. H04L 12/46
H04L 12/56

(21)Application number : 2001-193090
(22)Date of filing : 26.06.2001

(71)Applicant : NEC CORP
(72)Inventor : ONAWA YOICHI

(54) REMOTE VPN AUTHENTICATION AND MANAGEMENT SYSTEM, AND CONSTRUCTING METHOD OF THE SAME

(57)Abstract:
PROBLEM TO BE SOLVED: To provide integrated virtual private network (VPN) service management and operation which have not been performed because a VPN is established, managed and operated in each link, and to provide unified tunnel server operation and management in communication with plural ISPs.
SOLUTION: In a server which is established between a group of clients and a group of Internet service providers and remotely authenticates and manages a group of VPN converters to provide end-to-end VPN service, this remote VPN authentication and management server is featured in that it has a means to issue an authentication certificate, a means to control communication, a means to collect status information, a means to collect traffic statistics information, a means to monitor and control faults, a means to analyze statistics information, and a means to report to each client.



LEGAL STATUS

[Date of request for examination] 28.05.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－8607
（P2003－8607A）
(43)公開日　平成15年１月10日(2003.1.10)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　12/46	Ｍ	５Ｋ０３０
12/56	４００	12/56	４００Ｚ	５Ｋ０３３

審査請求　有　　請求項の数11　ＯＬ　（全 14 頁）

(21)出願番号　特願2001－193090(P2001－193090)

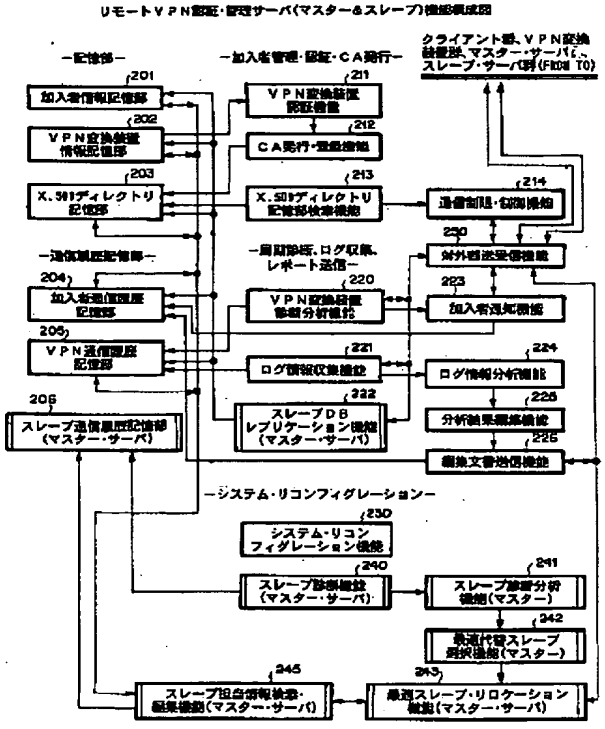
(22)出願日　平成13年６月26日(2001.6.26)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　大縄　陽一
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100065385
弁理士　山下　穣平

Ｆターム(参考)　5K030 GA11 GA15 HA04 JA10 MB09 MC07
5K033 BA08 DA05 DB20 EA07

(54)【発明の名称】　リモートＶＰＮ認証・管理システムおよびリモートＶＰＮ認証・管理システム構築方法

(57)【要約】
【課題】　ＶＰＮはリンク･バイ・リンクで設定され管理運用される為、統合的ＶＰＮサービスの管理運営が成されないという問題と複数のＩＳＰにまたがる通信においては、トンネルサーバの運営管理が一元的に成されていないという問題があった。
【解決手段】　クライアント群とＩＳＰ（internet service provider）群との間に設置され、エンド・ツー・エンドのＶＰＮ（virtual private network）サービスを提供するＶＰＮ変換装置群をリモートから認証・管理サービスを提供するサーバにおいて、認証証発行手段と、通信を制御する手段と、ステータス情報収集手段と、トラフィック統計情報収集手段と、障害監視制御手段と、統計情報分析手段と、各クライアントにレポーティング手段と、を備えることを特徴とするリモートＶＰＮ認証・管理サーバの提供。



【特許請求の範囲】
【請求項１】　クライアント群とＩＳＰ（internet service provider）群との間に設置され、エンド・ツー・エンドのＶＰＮ（virtual private network）サービスを提供するＶＰＮ変換装置群をリモートから認証・管理サービスを提供するサーバにおいて、
前記クライアント群からのサービス提供への加入申請情報を受付・審査後、審査結果を前記クライアント群に通知する手段と、
前記審査結果でサービス提供可能と判定された前記クライアント群からの前記申請情報を第１の記憶部に前記クライアント毎に登録する手段と、
前記審査結果でサービス提供可能と判定された前記クライアント群が使用する前記ＶＰＮ変換装置群の情報を前記第１の記憶部に前記クライアント毎に登録する手段と、
前記登録されたクライアント群との通信内容の履歴を第２の記憶部に前記クライアント毎に登録する手段と、
前記登録されたＶＰＮ変換装置との通信内容の履歴を第３の記憶部に前記ＶＰＮ変換装置毎に登録する手段と、
前記加入登録されたクライアントが加入申請時、通信宛先の情報を申請した場合、通信宛先情報を第４の記憶部に前記クライアント毎に登録する手段と、
前記登録されたＶＰＮ変換装置群から認証証の発行要求があった場合、前記ＶＰＮ変換装置群に認証証を発行する手段と、
前記認証証が発行されたＶＰＮ変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第４の記憶部に前記クライアント毎に登録された通信宛先情報を検索する手段と、
前記検索結果を前記ＶＰＮ変換装置群に通知する手段と、
前記認証証が発行されたＶＰＮ変換装置群からステータス情報を収集する手段と、
前記認証証が発行されたＶＰＮ変換装置群でロギングしているトラフィックに関する統計情報を、前記認証証が発行されたＶＰＮ変換装置群から所定周期で収集する手段と、
前記認証証が発行されたＶＰＮ変換装置群に所定周期のプローブを送信し障害の監視制御を行う手段と、
前記認証証が発行されたＶＰＮ変換装置群から収集したトラフィックに関する統計情報を分析する手段と、
前記分析結果を前記認証証が発行された前記各クライアント群にレポーティングする手段と、
を備えることを特徴とするリモートＶＰＮ認証・管理サーバ。
【請求項２】　WWWブラウザを具備したクライアント群とＩＳＰ（internet service provider）群との間に設置され、エンド・ツー・エンドのＶＰＮ（virtual private network）サービスを提供するＶＰＮ変換装置群をリモートから認証・管理サービスを提供するシステムにおいて、
前記クライアント群からのサービス提供の加入申請を受付・審査後、前記審査結果を前記クライアント群に通知する手段と、
前記審査結果でサービス可能と判定された前記クライアント群からの前記加入申請情報を第１の記憶部に前記クライアント毎に登録する手段と、
前記審査結果でサービス可能と判定された前記クライアント群が使用する前記ＶＰＮ変換装置群の情報を前記第１の記憶部に前記クライアント毎に登録する手段と、
前記登録されたクライアント群との通信内容の履歴を第２の記憶部に前記クライアント毎に登録する手段と、
前記登録されたＶＰＮ変換装置群との通信内容の履歴を第３の記憶部に前記ＶＰＮ変換装置毎に登録する手段と、
前記クライアント群が加入申請時に申請した通信アクセス宛先情報を記憶する第４の記憶部に前記クライアント毎に登録する手段と、
前記登録されたＶＰＮ変換装置群から認証証の発行要求があった場合、前記ＶＰＮ変換装置群に認証証を発行する手段と、
前記認証証が発行されたＶＰＮ変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第４の記憶部に前記クライアント毎に登録された前記通信宛先情報を検索する手段と、
前記検索結果を前記認証証が発行されたＶＰＮ変換装置群に通知する手段と、
前記認証証が発行されたＶＰＮ変換装置群からステータス情報を収集する手段と、
前記認証証が発行されたＶＰＮ変換装置群でロギングしているトラフィックに関する統計情報を、前記認証証が発行されたＶＰＮ変換装置群から所定周期で収集する手段と、
前記認証証が発行されたＶＰＮ変換装置群に所定周期のプローブを送信し障害の監視制御を行う手段と、
前記認証証が発行されたＶＰＮ変換装置群から収集したトラフィックに関する統計情報を分析する手段と、
前記分析結果を前記認証証が発行された前記各クライアント群に所定周期でレポーティング情報を編集する手段と、
前記所定周期で編集した文書情報を電子メールにハイパーリンクする手段と、
前記電子メールに前記第１の記憶部にある前記クライアント群のメールアドレスを付加する手段と、
前記電子メールを所定周期で送信する手段と、
前記電子メールを所定周期で受信したクライアント群が前記文章情報を開くとWWWブラウザに前記レポーティング内容が表示される手段と、
を備えることを特徴とするリモートＶＰＮ認証・管理サ

ーバ。

【請求項３】　請求項２に記載のリモートＶＰＮ認証・管理サーバにおいて、

地理的条件と前記認証証が発行されたＶＰＮ変換装置群を管理する数とにより、マスター・サーバとスレーブ・サーバ群とで負荷分散による分散システム構成とする手段と、

前記マスター・サーバで前記マスター・サーバと前記スレーブ・サーバ群との通信の履歴を第５の記憶部に前記スレーブ・サーバ毎に登録する手段と、

前記マスター・サーバが前記スレーブ・サーバからの確認応答をとる場合には前記マスター・サーバにおいて、前記スレーブ・サーバ群からの確認応答に対し、ワン・タイム・パスワードで認証する手段と、

前記マスター・サーバからスレーブ・サーバ群にステータス情報の問い合わせを所定周期で行い前記スレーブ・サーバ群からの確認応答に対し、前記マスター・サーバで前記ワン・タイム・パスワードで認証する手段と、

前記応答の結果、無応答または障害のステータス情報を添付した前記スレーブ・サーバがあった場合、前記マスター・サーバにおいて最適代替えスレーブ・サーバの選択手段と、

前記選択された代替スレーブ・サーバに対し、前記マスター・サーバから、前記スレーブ・サーバが管理対象とする前記認証証が発行されたＶＰＮ変換装置に関する前記第１の記憶部、第２の記憶部、第３の記憶部および第４の記憶部の関連情報を送信し確認応答をとる手段と、

前記スレーブ・サーバ群には、前記第１の記憶部、第２の記憶部、第３の記憶部および第４の記憶部の内容をマスター・サーバで一元管理する為のレプリケーション手段と、

を備えることを特徴とするリモートＶＰＮ認証・管理サーバ。

【請求項４】　クライアント群とＩＳＰ（internet service provider）群との間に設置され、エンド・ツー・エンドのＶＰＮ（virtual private network）サービスを提供するＶＰＮ変換装置群をリモートから認証・管理サービスを提供する方法において、

前記クライアント群からのサービス提供への加入申請を受付・審査後、前記審査結果を前記クライアント群に通知するステップと、

前記審査結果でサービス提供可能と判定された前記クライアント群からの前記申請情報を第１の記憶部に前記クライアント毎に登録するステップと、

前記審査結果でサービス提供可能と判定された前記クライアント群が使用する前記ＶＰＮ変換装置群の情報を前記第１の記憶部に前記クライアント毎に登録するステップと、

前記登録されたクライアント群との通信内容の履歴を第２の記憶部に前記クライアント毎に登録するステップと、

前記登録されたＶＰＮ変換装置群との通信内容の履歴を第３の記憶部に前記ＶＰＮ変換装置毎に登録するステップと、

前記クライアントが加入申請時、通信宛先情報を申請した場合、前記通信宛先情報を第４の記憶部に前記クライアント毎に登録するステップと、

前記登録されたＶＰＮ変換装置群から認証証の発行要求があった場合、前記ＶＰＮ変換装置群とに認証証を発行するステップと、

前記認証証が発行されたＶＰＮ変換装置群から通信宛先への通信の可否について問合せがあった場合、前記通信宛先で前記第４の記憶部に前記クライアント毎に登録された前記通信可能宛先情報を検索するステップと、

前記検索結果を前記ＶＰＮ変換装置群に通知するステップと、

前記認証証が発行されたＶＰＮ変換装置群からステータス情報を収集するステップと、

前記認証証が発行されたＶＰＮ変換装置群でロギングしているトラフィックに関する統計情報を、前記認証証が発行されたＶＰＮ変換装置群から所定周期で収集するステップと、

前記認証証が発行されたＶＰＮ変換装置群に所定周期のプローブを送信し障害の監視制御を行うステップと、

前記認証証が発行されたＶＰＮ変換装置群から収集したトラフィックに関する統計情報を分析するステップと、

前記分析結果を前記認証証が発行された前記各クライアント群にレポーティングするステップと、

を備えることを特徴とするリモートＶＰＮ認証・管理サービス提供方法。

【請求項５】　WWWブラウザを具備したクライアント群とＩＳＰ（internet service provider）群との間に設置され、エンド・ツー・エンドのＶＰＮ（virtual private network）サービスを提供するＶＰＮ変換装置群をリモートから認証・管理サービスを提供する方法において、

前記クライアント群からのサービス提供の加入申請を受付・審査後、前記審査結果を前記クライアント群に通知するステップと、

前記審査結果でサービス可能と判定された前記クライアント群からの前記加入申請情報を第１の記憶部に前記クライアント毎に登録するステップと、

前記審査結果でサービス可能と判定された前記クライアント群が使用する前記ＶＰＮ変換装置群の情報を前記第１の記憶部に前記クライアント毎に登録するステップと、

前記登録されたクライアント群との通信内容の履歴を第２の記憶部に前記クライアント毎に登録するステップと、

前記登録されたＶＰＮ変換装置との通信内容の履歴を第

３の記憶部に前記ＶＰＮ変換装置毎に登録するステップと、
前記クライアントが加入申請時、通信宛先を申請した場合、前記通信宛先情報を第４の記憶部に前記クライアント毎に登録するステップと、
前記登録されたＶＰＮ変換装置群から認証証の発行要求があった場合、前記クライアント群と前記ＶＰＮ変換装置群とに認証証を発行するステップと、
前記認証証が発行されたＶＰＮ変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第４の記憶部に前記クライアント毎に登録された前記通信宛先情報を検索するステップと、
前記検索結果を前記認証証が発行されたＶＰＮ変換装置群に通知するステップと、
前記認証証が発行されたＶＰＮ変換装置群からステータス情報を収集するステップと、
前記認証証が発行されたＶＰＮ変換装置群でロギングしているトラフィックに関する統計情報を、前記認証証が発行されたＶＰＮ変換装置群から所定周期で収集するステップと、
前記認証証が発行されたＶＰＮ変換装置群に所定周期のプローブを送信し障害の監視制御を行うステップと、
前記認証証が発行されたＶＰＮ変換装置群から収集したトラフィックに関する統計情報を分析するステップと、
前記分析結果を前記認証証が発行された前記各クライアント群に所定周期でレポーティング情報を編集するステップと、
前記所定周期で編集した文書情報を電子メールにハイパーリンクするステップと、
前記電子メールに前記第１の記憶部にある前記クライアント群のメールアドレスを付加するステップと、
前記電子メールを所定周期で送信するステップと、
前記電子メールを所定周期で受信したクライアント群が前記文章情報を開くとWWWブラウザに前記レポーティング内容が表示されるステップと、
を備えることを特徴とするリモートＶＰＮ認証・管理サービス提供方法。
【請求項６】　請求項５に記載のリモートＶＰＮ認証・管理サービス提供方法において、
地理的条件と前記認証証が発行されたＶＰＮ変換装置群を管理する数とにより、マスター・サーバとスレーブ・サーバ群とで負荷分散による分散サーバ構成とするステップと、
前記マスター・サーバで前記マスター・サーバと前記スレーブ・サーバとの通信の履歴を第５の記憶部に前記スレーブ・サーバ毎に登録するステップと、
前記マスター・サーバが前記スレーブ・サーバからの確認応答をとる場合には前記マスター・サーバにおいて、
前記スレーブ・サーバ群からの確認応答に対し、ワン・タイム・パスワードで認証するステップと、
前記マスター・サーバからスレーブ・サーバ群にステータス情報の問い合わせを所定周期で行い前記スレーブ・サーバ群からの確認応答に対し、前記マスター・サーバで前記ワン・タイム・パスワードで認証するステップと、
前記応答の結果、無応答または障害のステータス情報を添付した前記スレーブ・サーバがあった場合、前記マスター・サーバにおいて、最適代替えスレーブ・サーバの選択ステップと、
前記選択された代替スレーブ・サーバに対し、前記マスター・サーバから、前記スレーブ・サーバが管理対象とする前記認証証が発行されたＶＰＮ変換装置に関する前記第１の記憶部、第２の記憶部、第３の記憶部および第４の記憶部の関連情報を送信し確認応答をとるステップと、
前記スレーブ・サーバ群には、前記第１の記憶部、第２の記憶部、第３の記憶部および第４の記憶部の内容をマスター・サーバで一元管理する為のレプリケーションステップと、
を備えることを特徴とするリモートＶＰＮ認証・管理サービス提供方法。
【請求項７】　クライアント群とＩＳＰ（internet service provider）群との間に設置され、エンド・ツー・エンドのＶＰＮ（virtual private network）サービスを提供するＶＰＮ変換装置群をリモートから認証・管理サービスを提供する方法をコンピュータに実行させるためのプログラムにおいて、前記方法は、
前記クライアント群からのサービス提供への加入申請情報を受付・審査後、前記審査結果を前記クライアント群に通知するステップと、
前記審査結果でサービス提供可能と判定された前記クライアント群からの前記申請情報を第１の記憶部に前記クライアント毎に登録するステップと、
前記審査結果でサービス提供可能と判定された前記クライアント群が使用する前記ＶＰＮ変換装置群の情報を前記第１の記憶部に前記クライアント毎に登録するステップと、
前記登録されたクライアント群との通信内容の履歴を第２の記憶部に前記クライアント毎に登録するステップと、
前記登録されたＶＰＮ変換装置との通信内容の履歴を第３の記憶部に前記ＶＰＮ変換装置毎に登録するステップと、
前記クライアントが加入申請時、通信宛先情報を申請した場合、前記通信宛先情報を第４の記憶部に前記クライアント毎に登録するステップと、
前記登録されたＶＰＮ変換装置群から認証証の発行要求があった場合、前記クライアント群と前記ＶＰＮ変換装置群とに認証証を発行するステップと、
前記認証証が発行されたＶＰＮ変換装置群から通信宛先

への通信の可否についての問合せがあった場合、前記通信宛先で前記第１の記憶部に登録された前記通信宛先情報を検索するステップと、
前記検索結果を前記ＶＰＮ変換装置群に通知するステップと、
前記認証証が発行されたＶＰＮ変換装置群からステータス情報を収集するステップと、
前記認証証が発行されたＶＰＮ変換装置群でロギングしているトラフィックに関する統計情報を、前記認証証が発行されたＶＰＮ変換装置群から所定周期で収集するステップと、
前記認証証が発行されたＶＰＮ変換装置群に所定周期のプローブを送信し障害の監視制御を行うステップと、
前記認証証が発行されたＶＰＮ変換装置群から収集したトラフィックに関する統計情報を分析するステップと、
前記分析結果を前記認証証が発行された前記各クライアント群にレポーティングするステップと、
を備えることを特徴とするプログラム。
【請求項８】　WWWブラウザを具備したクライアント群とＩＳＰ（internet service provider）群との間に設置され、エンド・ツー・エンドのＶＰＮ（virtual private network）サービスを提供するＶＰＮ変換装置群をリモートから認証・管理サービスを提供する方法をコンピュータに実行させるためのプログラムにおいて、前記方法は、
前記クライアント群からのサービス提供の加入申請を受付・審査後、前記審査結果を前記クライアント群に通知するステップと、
前記審査結果でサービス可能と判定された前記クライアント群からの前記加入申請情報を第１の記憶部に前記クライアント毎に登録するステップと、
前記審査結果でサービス可能と判定された前記クライアント群が使用する前記ＶＰＮ変換装置群の情報を前記第１の記憶部に前記クライアント毎に登録するステップと、
前記登録されたクライアント群との通信内容の履歴を第２の記憶部に前記クライアント毎に登録するステップと、
前記登録されたＶＰＮ変換装置との通信内容の履歴を第３の記憶部に前記ＶＰＮ変換装置毎に登録するステップと、
前記クライアントが加入申請時、通信宛先情報を申請した場合、前記通信宛先情報を第４の記憶部に前記クライアント毎に登録するステップと、
前記登録されたＶＰＮ変換装置群から認証証の発行要求があった場合、前記クライアント群と前記ＶＰＮ変換装置群とに認証証を発行するステップと、
前記認証証が発行されたＶＰＮ変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第１の記憶部に登録された前記通信宛先情報を検索するステップと、
前記検索結果を前記認証証が発行されたＶＰＮ変換装置群に通知するステップと、
前記認証証が発行されたＶＰＮ変換装置群からステータス情報を収集するステップと、
前記認証証が発行されたＶＰＮ変換装置群でロギングしているトラフィックに関する統計情報を、前記認証証が発行されたＶＰＮ変換装置群から所定周期で収集するステップと、
前記認証証が発行されたＶＰＮ変換装置群に所定周期のプローブを送信し障害の監視制御を行うステップと、
前記認証証が発行されたＶＰＮ変換装置群から収集したトラフィックに関する統計情報を分析するステップと、
前記分析結果を前記認証証が発行された前記各クライアント群に所定周期でレポーティング情報を編集するステップと、
前記所定周期で編集した文書情報を電子メールにハイパーリンクするステップと、
前記電子メールに前記第１の記憶部にある前記クライアント群のメールアドレスを付加するステップと、
前記電子メールを所定周期で送信するステップと、
前記電子メールを所定周期で受信したクライアント群が前記文章情報を開くとWWWブラウザに前記レポーティング内容が表示されるステップと、
を備えることを特徴とするプログラム。
【請求項９】　請求項８に記載のリモートＶＰＮ認証・管理サービス提供方法をコンピュータに実行させるためのプログラムにおいて、前記方法は、
地理的条件と前記認証証が発行されたＶＰＮ変換装置群を管理する数とにより、マスター・サーバとスレーブ・サーバ群とで負荷分散による分散サーバ構成とするステップと、
前記マスター・サーバで前記マスター・サーバとスレーブ・サーバとの通信の履歴を第５の記憶部に前記スレーブ・サーバ毎に登録するステップと、
前記マスター・サーバが前記スレーブ・サーバからの確認応答をとる場合には前記マスター・サーバにおいて、前記スレーブ・サーバ群からの確認応答に対し、ワン・タイム・パスワードで認証するステップと、
前記マスター・サーバからスレーブ・サーバ群にステータス情報の問い合わせを所定周期で行い前記スレーブ・サーバ群からの確認応答に対し、前記マスター・サーバが前記ワン・タイム・パスワードで認証するステップと、
前記応答の結果、無応答または障害のステータス情報を添付した前記スレーブ・サーバがあった場合、前記マスター・サーバにおいて、最適代替えスレーブ・サーバの選択ステップと、
前記選択された代替スレーブ・サーバに対し、前記マスター・サーバから、前記スレーブ・サーバが管理対象と

する前記認証証が発行されたＶＰＮ変換装置に関する前記第１の記憶部、第２の記憶部、第３の記憶部および第４の記憶部の関連情報を送信し確認応答をとるステップと、
前記スレーブ・サーバ群には、前記第１の記憶部、第２の記憶部、第３の記憶部および第４の記憶部の内容をマスター・サーバで一元管理する為のレプリケーションステップと、
を備えることを特徴とするプログラム。
【請求項１０】　ネットワークで相互に接続された、請求項１又は請求項２に記載のサーバと、前記ＶＰＮ変換装置群と、前記クライアント端末群と、を備えるリモートＶＰＮ認証・管理システムにおいて、
前記ＶＰＮ変換装置は、
前記サーバに対し認証証の発行要求を送信する手段と、
前記サーバから返信された認証証を記憶する手段と、
前記クライアントからのアクセス要求があった場合、サーバに対し通信の可否を問い合わせる手段と、
前記問い合わせの結果、通信を制限する返信を受信した場合、前記クライアントからの通信要求を拒絶する手段と、
前記問い合わせの結果、通信可能である旨の返信を受信した場合、前記クライアントに前記ＶＰＮサービスを提供する手段と、
前記サーバからのステータス問い合わせに対し、ステータス情報を返送する手段と、
前記クライアントへ又はからの通信の履歴を記憶部に登録する手段と、
前記サーバから通信のログ情報の要求を受信時、前記記憶部のクライアントに関する通信のログ情報を返送する手段と、を備え、
前記クライアント端末は、
前記ＶＰＮ通信手段と、
を備えることを特徴とするリモートＶＰＮ認証・管理システム。
【請求項１１】　請求項１０に記載のリモートＶＰＮ認証・管理システムにおいて、
前記ＶＰＮ変換装置は、
前記問い合わせの結果、通信可能である旨の返信を受信した場合、通信相手先の前記認証証が発行されたＶＰＮ変換装置との間で暗号化方式等のネゴシエーションを行う機能と、
を更に備え、
前記クライアント端末は、
前記クライアント端末が通信する宛先の前記ＶＰＮ変換装置との間でＶＰＮ通信の為の暗号化方式等のネゴシエーション手段と、を更に備えることを特徴とするリモートＶＰＮ認証・管理システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
【０００２】
【従来の技術】特開２０００－３４１３２７号公報には、ＶＰＮ構成方式、インターワークルータ装置、パケット通信方式、データ通信装置およびパケット中継装置について、複数のインターネットプロバイダ（ＩＳＰ）にまたがる仮想専用線（ＶＰＮ）を提供する方式として、ＩＳＰの入口と出口とに、各々ＶＰＮ変換システムを配備することにより、複数のＩＳＰにまたがるＶＰＮサービスを実現する例が示されている。
【０００３】特開２０００－２４４５４７号公報には、移動端末の認証方式およびＶＰＮの通信方式として、ポータルサイトにアクセス時に付与される秘密鍵情報により、ＶＰＮを管理しているサーバにアクセスすることにより、異なるネットワーク間にまたがるＶＰＮ通信の方式について述べている。
【０００４】特開２０００－５９３５７号公報には、ＶＰＮサービス構築の方法として、管理サーバにネットワークの使用クライアントのＩＤ番号、パスワードを登録し、各クライアントには認証・暗号化ソフトウェアを記憶させたＩＣカードを配布し、アクセス時、管理サーバにて認証およびクライアントを使用できるＶＰＮに割り当てることにより、ＶＰＮサービスを提供する方式について述べている。
【０００５】
【発明が解決しようとする課題】しかしながら、従来の方式には以下の問題点がある。
【０００６】特開２０００－３４１３２７号公報における、ＶＰＮ構成方式、インターワークルータ装置、パケット通信方式、データ通信装置およびパケット中継装置においては、ＶＰＮはリンク･バイ・リンクで設定され管理運用される為、統合的ＶＰＮサービスの管理運営が成されないという第１の問題があった。
【０００７】又、特開２０００－２４４５４７号公報における、移動端末の認証方式およびＶＰＮの通信方式においては、クライアントにＩＣカードを配布し、クライアントの端末には、ＩＣカード・リーダ等の設備を必要とすると共に複数のＩＳＰにまたがる通信においては、トンネルサーバの運営管理が一元的に成されていないという第２の問題があった。
【０００８】本発明は、これらの問題に鑑み発明されたものであり、統合的ＶＰＮサービスの提供を行う運営管理方式およびシステムを提供することを第１の目的とする。
【０００９】また、ＶＰＮサービスを提供するＶＰＮ変換装置の一元的管理・運営を行うサービスを提供することを第２の目的とする。
【００１０】
【課題を解決するための手段】本発明の第１の観点によれば、クライアント群とＩＳＰ（internet service pro

vider）群との間に設置され、エンド・ツー・エンドのＶＰＮ（virtual private network）サービスを提供するＶＰＮ変換装置群をリモートから認証・管理サービスを提供するサーバにおいて、前記クライアント群からのサービス提供への加入申請情報を受付・審査後、前記審査結果を前記クライアント群に通知する手段と、前記審査結果でサービス提供可能と判定された前記クライアント群からの前記申請情報を第１の記憶部に前記クライアント毎に登録する手段と、前記審査結果でサービス提供可能と判定された前記クライアント群が使用する前記ＶＰＮ変換装置群の情報を前記第１の記憶部に前記クライアント毎に登録する手段と、前記登録されたクライアント群との通信内容の履歴を第２の記憶部に前記クライアント毎に登録する手段と、前記登録されたＶＰＮ変換装置との通信内容の履歴を第３の記憶部に前記ＶＰＮ変換装置毎に登録する手段と、前記登録されたＶＰＮ変換装置群から認証証の発行要求があった場合、前記クライアントが加入申請時、通信宛先情報を申請した場合、前記通信宛先情報を第４の記憶部に前記クライアント毎に登録する手段と、前記ＶＰＮ変換装置群に認証証を発行する手段と、前記認証証が発行されたＶＰＮ変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第４の記憶部に登録された前記通信宛先情報を検索する手段と、前記検索結果を前記ＶＰＮ変換装置群に通知する手段と、前記認証証が発行されたＶＰＮ変換装置群からステータス情報を収集する手段と、前記認証証が発行されたＶＰＮ変換装置群でロギングしているトラフィックに関する統計情報を、前記認証証が発行されたＶＰＮ変換装置群から所定周期で収集する手段と、前記認証証が発行されたＶＰＮ変換装置群に所定周期のプローブを送信し障害の監視制御を行う手段と、前記認証証が発行されたＶＰＮ変換装置群から収集したトラフィックに関する統計情報を分析する手段と、前記分析結果を前記認証証が発行された前記各クライアント群にレポーティングする手段と、を備えることを特徴とするリモートＶＰＮ認証・管理サーバが提供される。

【００１１】本発明の第２の観点によれば、WWWブラウザを具備したクライアント群とＩＳＰ（internet service provider）群との間に設置され、エンド・ツー・エンドのＶＰＮ（virtual private network）サービスを提供するＶＰＮ変換装置群をリモートから認証・管理サービスを提供するシステムにおいて、前記クライアント群からのサービス提供の加入申請情報を受付・審査後、前記審査結果を前記クライアント群に通知する手段と、前記審査結果でサービス可能と判定された前記クライアント群からの前記加入申請情報を第１の記憶部に前記クライアント毎に登録する手段と、前記審査結果でサービス可能と判定された前記クライアント群が使用する前記ＶＰＮ変換装置群の情報を前記第１の記憶部に前記クライアント毎に登録する手段と、前記登録されたクライアント群との通信内容の履歴を第２の記憶部に前記クライアント毎に登録する手段と、前記登録されたＶＰＮ変換装置との通信内容の履歴を第３の記憶部に前記ＶＰＮ変換装置毎に登録する手段と、前記クライアントが加入申請時、通信宛先情報を申請した場合、前記通信宛先情報を第４の記憶部に前記クライアント毎に登録する手段と、前記登録されたＶＰＮ変換装置群から認証証の発行要求があった場合、前記クライアント群と前記ＶＰＮ変換装置群とに認証証を発行する手段と、前記認証証が発行されたＶＰＮ変換装置群から通信宛先への通信の可否についての問合せがあった場合、前記通信宛先で前記第４の記憶部に登録された前記通信宛先情報を検索する手段と、前記検索結果を前記認証証が発行されたＶＰＮ変換装置群に通知する手段と、前記認証証が発行されたＶＰＮ変換装置群からステータス情報を収集する手段と、前記認証証が発行されたＶＰＮ変換装置群でロギングしているトラフィックに関する統計情報を、前記認証証が発行されたＶＰＮ変換装置群から所定周期で収集する手段と、前記認証証が発行されたＶＰＮ変換装置群に所定周期のプローブを送信し障害の監視制御を行う手段と、前記認証証が発行されたＶＰＮ変換装置群から収集したトラフィックに関する統計情報を分析する手段と、前記分析結果を前記認証証が発行された前記各クライアント群に所定周期でレポーティング情報を編集する手段と、前記所定周期で編集した文書情報を電子メールにハイパーリンクする手段と、前記電子メールに前記第１の記憶部にある前記クライアント群のメールアドレスを付加する手段と、前記電子メールを所定周期で送信する手段と、前記電子メールを所定周期で受信したクライアント群が前記文章情報を開くとWWWブラウザに前記レポーティング内容が表示される手段と、を備えることを特徴とするリモートＶＰＮ認証・管理サーバが提供される。

【００１２】前記リモートＶＰＮ認証・管理サーバは、地理的条件と前記認証証が発行されたＶＰＮ変換装置群を管理する数とにより、マスター・サーバとスレーブ・サーバ群とで負荷分散による分散システム構成とする手段と、前記マスター・サーバで前記マスター・サーバとスレーブ・サーバとの通信の履歴を第５の記憶部に前記スレーブ・サーバ毎に登録する手段と、前記マスター・サーバが前記スレーブ・サーバからの確認応答をとる場合には前記マスター・サーバにおいて、前記スレーブ・サーバ群からの確認応答に対し、ワン・タイム・パスワードで認証する手段と、前記マスター・サーバからスレーブ・サーバ群にステータス情報の問い合わせを所定周期で行い前記スレーブ・サーバ群からの確認応答に対し、前記マスター・サーバで前記ワン・タイム・パスワードで認証する手段と、前記応答の結果、無応答または障害のステータス情報を添付した前記スレーブ・サーバ

があった場合、前記マスター・サーバにおいて、最適代替えスレーブ・サーバの選択手段と、前記選択された代替スレーブ・サーバに対し、前記マスター・サーバから、前記スレーブ・サーバが管理対象とする前記認証証が発行されたＶＰＮ変換装置に関する前記第１の記憶部、第２の記憶部、第３の記憶部および第４の記憶部の関連情報を送信し確認応答をとる手段と、前記スレーブ・サーバ群には、前記第１の記憶部、第２の記憶部、第３の記憶部および第４の記憶部の内容をマスター・サーバで一元管理する為のレプリケーション手段と、を更に備えてもよい。

【００１３】本発明の第３の観点によれば、ネットワークで相互に接続された、前記サーバと、前記ＶＰＮ変換装置群と、前記クライアント端末群と、を備えるリモートＶＰＮ認証・管理システムにおいて、前記ＶＰＮ変換装置は、前記サーバに対し認証証の発行要求を送信する手段と、前記サーバから返信された認証証を記憶する手段と、前記クライアントからのアクセス要求があった場合、サーバに対し通信の可否を問い合わせる手段と、前記問い合わせの結果、通信を制限する返信を受信した場合、前記クライアントからの通信要求を拒絶する手段と、前記問い合わせの結果、通信可能である旨の返信を受信した場合、通信相手先の前記認証証が発行されたＶＰＮ変換装置との間で暗号化方式等のネゴシエーションを行う機能と、前記クライアントに前記ＶＰＮサービスを提供する手段と、前記サーバからのステータス問い合わせに対し、ステータス情報を返送する手段と、前記クライアントへ又はからの通信の履歴を記憶部に登録する手段と、前記サーバから通信の履歴情報の要求を受信時、前記記憶部のクライアントに関する通信履歴情報を返送する手段と、を備え、前記クライアント端末は、前記ＶＰＮ通信手段と、前記クライアント端末が通信する宛先の前記ＶＰＮ変換装置との間でＶＰＮ通信の為の暗号化方式等のネゴシエーション手段と、を備えることを特徴とするリモートＶＰＮ認証・管理システムが提供される。

【００１４】

【発明の実施の形態】実施の形態１について、図１から図４を用いて説明する。

【００１５】図１は、本発明のシステム構成を示しており、端末－Ｘ１０１、イントラネット－Ａ１０２、イントラネット－Ｂ１０３、イントラネット内の端末－Ａ、イントラネット内の端末－Ｂ１０５、VPN変換装置－Ａ１０６、VPN変換装置－Ｂ１０７、リモートVPN認証・管理サーバ（マスター）１０８、リモートVPN認証・管理サーバ（スレーブ）１０９、交換網１１０、ISP－Ａ１１１、ISP－Ｘ１１２、ワールドワイドインターネット１１３から構成される。

【００１６】図２は、リモートVPN認証・管理サーバにおける機能構成を示しており、加入者情報記憶部２０１、VPN変換装置情報記憶部２０２、X.509ディレクトリ記憶部２０３、加入者通信履歴記憶部２０４、VPN通信履歴記憶部２０５、スレーブ通信履歴記憶部（マスター・サーバ）２０６、ＶＰＮ変換装置認証機能２１１、CA発行・登録機能２１２、X.509ディレクトリ記憶部検索機能２１３、通信制限制御機能２１４、ＶＰＮ変換装置診断・分析機能２２０、ログ情報収集機能２２１、スレーブDBレプリケーション機能２２２、加入者通知機能２２３，ログ情報分析機能２２４、分析結果編集機能２２５、編集文書送信機能２２６、システム・リコンフィグレーション機能２３０、スレーブ診断機能（マスター・サーバ）２４０、スレーブ診断分析機能２４１、最適代替スレーブ選択機能（マスター・サーバ）２４２、最適スレーブ・リロケーション機能（マスター・サーバ）２４３、スレーブ担当情報検索・編集機能（マスター・サーバ）２４５、対外部送受信機能２５０から構成される。

【００１７】加入者情報記憶部２０１は、クライアントから加入申請があった場合、クライアントが設置したVPN変換装置がサービス提供対象の仕様を備えているか否かを審査し、サービス提供可能で有れば加入を認可し、クライアントが申請したクライアントのメールアドレス、クライアントが設置したVPN変換装置のIPアドレス、サービス料金決済方法、サーバーが登録時発行するクライアントのオーガニゼーション番号、ID番号、シグネチャ番号情報を記憶するクライアント毎に記憶する。

【００１８】VPN変換装置情報記憶部２０２は、CAを発行したVPN変換装置に関する情報をクライアント毎に記憶する。

【００１９】X.509ディレクトリ記憶部２０３は、クライアント別にアクセス可能な通信宛先情報を管理し、X.509に準拠したディレクトリー情報を記憶する。

【００２０】加入者通信履歴記憶部２０４は、CAを発行したクライアント群との通信の履歴情報をクライアント毎に記憶する。

【００２１】VPN通信履歴記憶部２０５は、CAを発行したVPN変換装置との通信履歴情報をVPN変換装置毎に記憶する。

【００２２】スレーブ通信履歴記憶部（マスター・サーバ）２０６は、マスター・サーバでスレーブ・サーバ群との通信の履歴を記憶する。

【００２３】ＶＰＮ変換装置認証機能２１１は、加入認可したVPN変換装置からのアクセス時、認証を行う。

【００２４】CA発行・登録機能２１２は、加入認可したVPN変換装置からのCA（認証証）要求に対し認証証を発行する。

【００２５】X.509ディレクトリ記憶部検索機能２１３は、VPN変換装置からの通信宛先への通信の可否の問い合わせに対し、通信宛先でX.５０９ディレクトリー記憶部２０３のクライアント毎の通信宛先情報を検索する。

【００２６】通信制限制御機能２１４は、X.５０９ディレクトリー記憶部検索の結果、通信の可否をVPN変換装置に返送する。

【００２７】ＶＰＮ変換装置診断・分析機能２２０は、CAを発行したVPN変換装置群に所定周期でプローブを送信し、ステータス情報をVPN変換装置から収集する。

【００２８】ログ情報収集機能２２１は、VPN変換装置でのトラフィック関連情報等のロギング情報を一定周期でVPN変換装置から収集する。

【００２９】スレーブDBレプリケーション機能２２２は、マスター・サーバで、各記憶部をマスター・サーバで一元管理するためにスレーブ・サーバでの各記憶部のレプリケーション機能を起動させる。

【００３０】加入者通知機能２２３は、VPN変換装置の診断・分析結果、異常と判断した場合、クライアントにその旨通知する。

【００３１】ログ情報分析機能２２４は、収集されたロギング情報を分析する。

【００３２】分析結果編集機能２２５は、各VPN変換装置でのロギング情報を分析した結果を各クライアント別に編集する。

【００３３】編集文書送信機能２２６は、各クライアント別に編集されたレポーティング情報をハイパーリンクし、各クライアントのメールアドレスを付加して送信する。

【００３４】システム・リコンフィグレーション機能２３０は、サーバ・システム内での障害発生時にシステム構成を自動的に再構成する。

【００３５】スレーブ診断機能（マスター・サーバ）２４０は、マスター・サーバでのスレーブ・サーバの状態情報を所定周期で収集する。

【００３６】スレーブ診断分析機能２４１は、スレーブ・サーバからのステータス情報を分析する。

【００３７】最適代替スレーブ選択機能（マスター・サーバ）２４２は、スレーブ・サーバの代替が必要な場合にマスター・サーバで最適な代替スレーブ・サーバを選択する。

【００３８】最適スレーブ・リロケーション機能（マスター・サーバ）２４３は、代替スレーブ・サーバが選択された場合、当該スレーブ・サーバに必要情報を再配置する。

【００３９】スレーブ担当情報検索・編集機能２４５は、マスター・サーバで代替スレーブ・サーバが選択された場合、当該スレーブ・サーバに必要情報を関連記憶部から検索・収集・編集する。

【００４０】対外部送受信機能２５０は、クライアント、ＶＰＮ変換装置、マスター・サーバ、スレーブ・サーバ群へ及びからの通信の送受信を行う。

【００４１】次に実施の形態１の動作について、図３及び図４を用いて説明する。

【００４２】図３において、クライアントからサービス加入申請があった場合（Ｓ３０１）、加入申請情報からサービス提供可能か否かを審査し不可の場合、審査結果を電子メールで通知する（Ｓ３０３）。サービス提供可能である場合には、各クライアントにオーガニゼーション番号、ID番号、シグネチャ番号（パスワード）を発行し送付（Ｓ３０２）し、クライアント毎に記憶するサービス加入者情報記憶部２０１に登録する。

【００４３】また、通信宛先情報はクライアント毎に登録管理するX.509ディレクトリー記憶部に登録される。

【００４４】審査の結果サービス提供可能であるとされ、オーガニゼーション番号、ID番号、シグネチャ番号（パスワード）が発行されたクライアントのVPN変換装置から、認証書（CA）の発行要求があった場合（Ｓ３１０）、オーガニゼーション番号、ID番号、シグネチャ番号（パスワード）で認証を行い、NGの場合にはその旨返信し（Ｓ３１２）、OKの場合には認証書をVPN変換装置に返送する（Ｓ３１１）。

【００４５】次に図４を用いて、一連の動作について説明する。

【００４６】CAを発行されたVPN変換装置から、クライアントからのアクセス要求（Ｓ４１０）に基づく通信宛先との通信の可否の問い合わせを受信した場合（Ｓ４２０）、オーガニゼーション番号、ID番号、シグネチャ番号（パスワード）で認証を行い、NGの場合にはその旨返信し（Ｓ４２１）、認証ＯＫの場合、各クライアント単位で登録管理するX.509ディレクトリー記憶部を通信宛先で検索し、通信宛先情報に登録されている宛先か否かを判定し、判定結果をVPN変換装置に返送し（Ｓ４２２）、通信の制限・制御を行う。

【００４７】次にリモートVPN変換装置認証・管理サーバから所定周期でCAを発行されたVPN変換装置群にステータス情報を収集するプローブを送信し（Ｓ４３０）、VPN変換装置群からのステータス情報を添付した返信を受信し（Ｓ４３１）、受信結果を分析し、ＶＰＮ変換装置に異常が認められた場合、クライアントにその旨通知し（Ｓ４３２）、VPN装置の障害等の監視を行う。

【００４８】次にリモートVPN変換装置認証・管理サーバから所定周期でCAを発行されたVPN変換装置群にVPN変換装置群でロギングしているトラフィック関連情報を収集する為のプローブを送信し（Ｓ４４０）、VPN変換装置群からVPN変換装置群でロギングしているトラフィック関連情報を添付した返信を受信し（Ｓ４４１）、VPN装置群のトラフィック関連情報を収集し、収集したトラフィック関連の統計情報を分析する。

【００４９】次に分析されたトラフィック関連情報は文書に編集し、各クライアントに編集された文章情報をハイパーリンクしたメールを送信し（Ｓ４４２）、メールを受信した各クライアントは、編集された文章情報を開くと自動的にWWWブラウザが起動され、編集された文章

情報にアクセスし（Ｓ４４３）、WWWブラウザの画面に編集された文章が表示される（Ｓ４４４）。

【００５０】第２の実施の形態について、図５を用いて説明する。

【００５１】図５に示すように、分散システム構成時、リモートＶＰＮ認証・管理スレーブ・サーバ群５０１に対し、マスター・サーバ１０８からステータス状況を問い合わせるプローブが所定周期で送信され（Ｓ５１０）、スレーブ・サーバ群５０１からのステータス情報を含む返信を受信する（Ｓ５１１）。

【００５２】次にスレーブ・サーバ群５０１からの返信情報に過負荷情報、障害情報又は無応答をマスター・サーバ１０８で検出した場合、マスター・サーバ１０８は最適な代替スレーブ・サーバを選定し、当該スレーブ・サーバに代替スレーブ指示を送信し（Ｓ５２１）、確認応答をとり（Ｓ５２２）、代替関連情報を当該スレーブ・サーバに送信し（Ｓ５２３）、確認応答（Ｓ５２４）を当該スレーブ・サーバからとることにより、提供サービスに切れ目の無いコンシステンシー・サービスを提供する。

【００５３】次にマスター・サーバ１０８で一元管理する為、所定周期でスレーブ・サーバ群５０１のレプリケーション機能にスレーブ・サーバの各記憶部の前回送信からの差分の送信要求（Ｓ５３０）を送信し、各記憶部の差分を受信（Ｓ５３１）する動作をすべてのスレーブ・サーバに対し行い、マスター・サーバ１０８の各記憶部を更新・登録することにより、一元的に全てのＶＰＮ変換装置及びサービス提供クライアント情報を管理する。

【００５４】第３の実施の形態について、図４及び図６を用いて説明する。

【００５５】図４に示した本発明の動作説明図におけるVPN変換装置群４０２、リモートVPN認証管理サーバ３０３についての動作については、図４に示した通りである。

【００５６】ここでは図６でのイントラネット内の端末－Ａ１０４とVPN変換装置－Ａ１０６及びVPN変換装置－Ｂ１０７を介したイントラネット内の端末－Ｂ１０５間での動作について図６にて説明する。

【００５７】図６において、ＶＰＮ変換装置にイントラネット内の端末－Ａ１０４からアクセス要求（Ｓ６１０）が有ると、図４に示したようにリモート認証管理サーバにアクセスの可否を問い合わせ、アクセス可の場合、宛先イントラネット内の端末－Ｂ１０５のＶＰＮ変換装置－Ｂ１０７にＶＰＮ変換装置－Ａ１０６からアクセス（Ｓ６１１）し、ＩＰsecに基づく暗号化方式等のネゴシエーション（Ｓ６１２）をＶＰＮ変換装置間（１０６、１０７）で行い（Ｓ６１２）、VPNセッション確立後、端末－Ａ１０４と端末－Ｂ１０５間でVPN通信（Ｓ６１３）を行う。

【００５８】次に、図７を用いて端末にVPN通信機能を搭載した場合での動作について説明する。

【００５９】図７において、端末－Ｘ１０１からISP－Ｘ１１２にダイアルアップ回線接続（Ｓ７１０）を行い予め加入契約したISP－Ｘ１１２の接続ポートと接続し、ID、パスワードの送信（Ｓ７１１）によりISP―Ｘ１１２から認証を受け、ＩＰアドレスが返送（Ｓ７１２）される。

【００６０】接続宛先端末－Ａ１０４のVPN変換装置－Ａ１０６に通信要求を送信（Ｓ７１３）し、ＩＰsecに基づく暗号化方式等のネゴシエーション（Ｓ７１４）をＶＰＮ変換装置－Ａ１０６との間で行いＶＰＮセッション確立後、ＶＰＮ通信（Ｓ７１５）にて端末－Ｘ１０１と端末－Ａ１０４の間でＶＰＮを使用した通信を行う。

【００６１】

【発明の効果】本発明の第１の効果は、エンド・ツー・エンドでシンプルかつメンテナンス・フリーなVPN変換装置の認証・管理サービスが提供されることである。

【００６２】本発明の第２の効果は、従来１つのISPに閉じられていたVPNサービスとその認証・管理に統合的なサービスが提供されることである。

【００６３】本発明の第３の効果は、従来１つのISPに閉じられていたVPNサービスとその認証・管理に一元的な管理サービスが提供されることである。

【００６４】本発明の第４の効果は、分散型システム構成をとることにより、信頼性の高いサービスが提供されることである。

【００６５】本発明の第５の効果は、また、分散型のシステムにより、VPN変換装置との間のトラフィックを軽減できることである。

【００６６】本発明の第６の効果は、分散型のシステム構成をとることにより、スレーブ・サーバの初期投資を軽減できることである。

【図面の簡単な説明】

【図１】本発明のシステム構成概要を示すシステム構成概要図である。

【図２】本発明のサーバでの機能構成と機能間の関連を示すシステム機能構成図である。

【図３】本発明のクライアントから加入申請を受けてから、CAを発行するまでのクライアント、VPN変換装置及びリモート認証管理サーバ間の動作を示すシーケンス図である。

【図４】本発明でのCAを発行されたクライアント、VPN変換装置及びリモート認証管理サーバ間の動作を示すシーケンス図である。

【図５】本発明のシステム構成を分散システム構成とした場合のマスター・サーバとスレーブ・サーバ群との動作を示すシーケンス図である。

【図６】本発明のVPN変換機能搭載の端末及びVPN変換装置を介したイントラネット内の端末間での通信でのシス

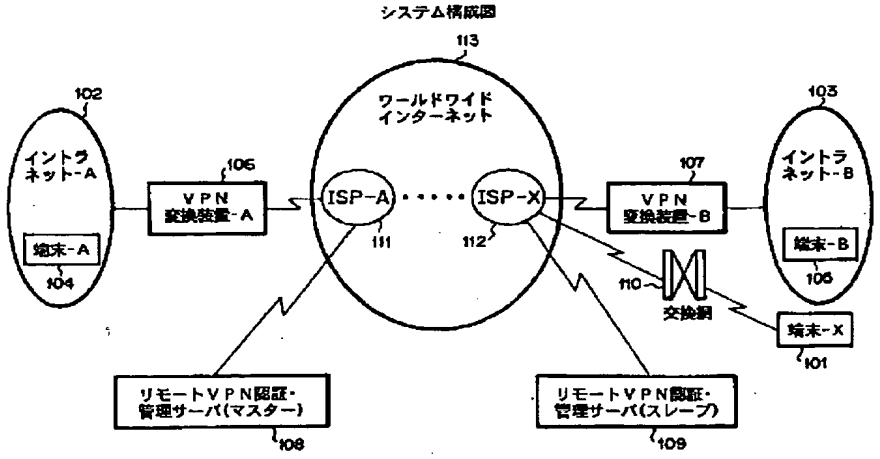
テム構成と各システムの動作を示すシーケンス図である。

【図７】本発明のイントラネット内の端末間でＶＰＮ通信を行う場合のシステム構成と各システムでの動作について示すシーケンス図である。

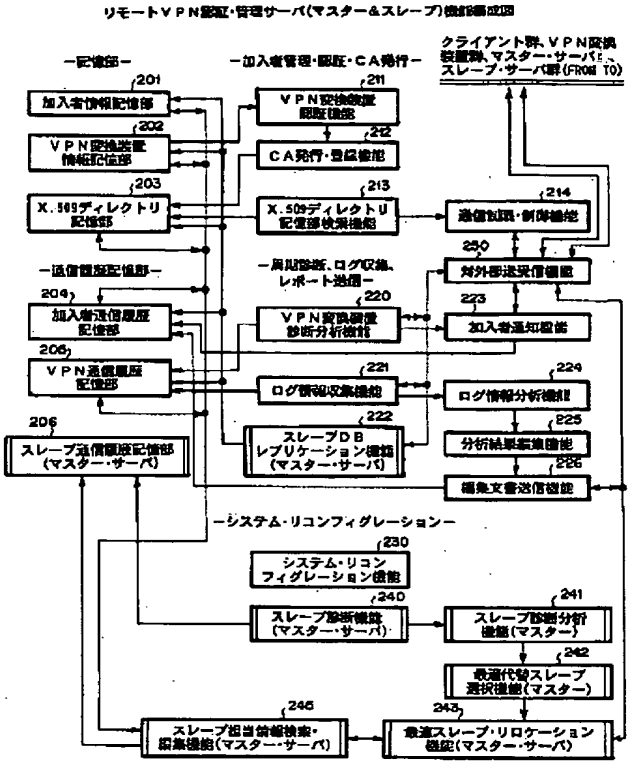
【符号の説明】

１０１　端末－Ｘ
１０２　イントラネット－Ａ
１０３　イントラネット－Ｂ
１０４　イントラネット内の端末－Ａ
１０５　イントラネット内の端末－Ｂ
１０６　VPN変換装置－Ａ
１０７　VPN変換装置－Ｂ
１０８　リモート認証管理サーバ（マスター・サーバ）
１０９　リモート認証管理サーバ（スレーブ・サーバ）
１１０　交換網
１１１　ISP－Ａ
１１２　ISP－Ｘ
１１３　ワールドワイドインターネット
２０１　加入者情報記憶部
２０２　VPN変換装置情報記憶部
２０３　X.509ディレクトリ記憶部
２０４　加入者通信履歴記憶部
２０５　VPN通信履歴記憶部
２０６　スレーブ通信履歴記憶部（マスター・サーバ）
２１１　ＶＰＮ変換装置認証機能
２１２　CA発行・登録機能
２１３　X.509ディレクトリ記憶部検索機能
２１４　通信制限制御機能
２２０　ＶＰＮ変換装置診断・分析機能
２２１　ログ情報収集機能
２２２　スレーブDBレプリケーション機能
２２３　加入者通知機能
２２４　ログ情報分析機能
２２５　分析結果編集機能
２２６　編集文書送信機能
２３０　システム・リコンフィグレーション機能
２４０　スレーブ診断機能（マスター・サーバ）
２４１　スレーブ診断分析機能
２４２　最適代替スレーブ選択機能（マスター・サーバ）
２４３　最適スレーブ・リロケーション機能（マスター・サーバ）
２４５　スレーブ担当情報検索・編集機能（マスター・サーバ）
２５０　対外部送受信機能
３０１　クライアント
３０２　ＶＰＮ変換装置
３０３　リモート認証管理サーバ
４０１　クライアント群
４０２　ＶＰＮ変換装置群
５０１　スレーブ・サーバ群

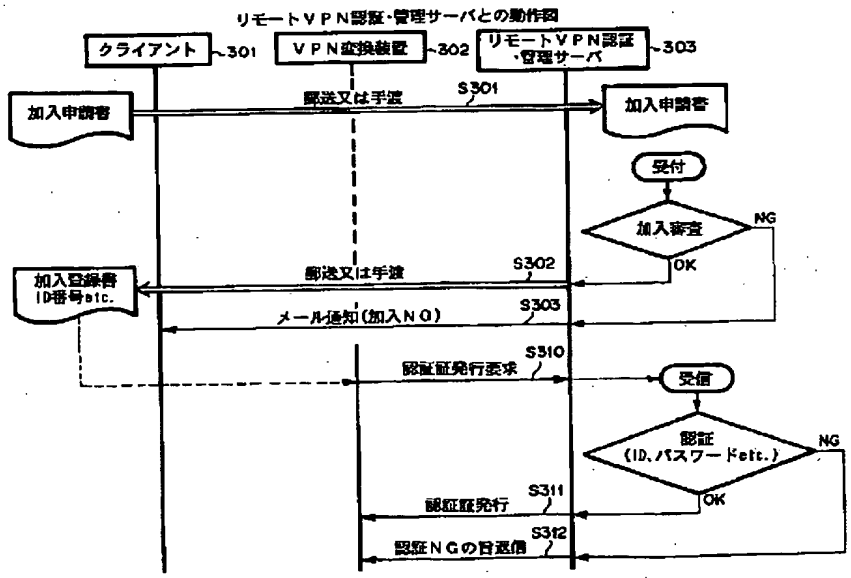
【図１】



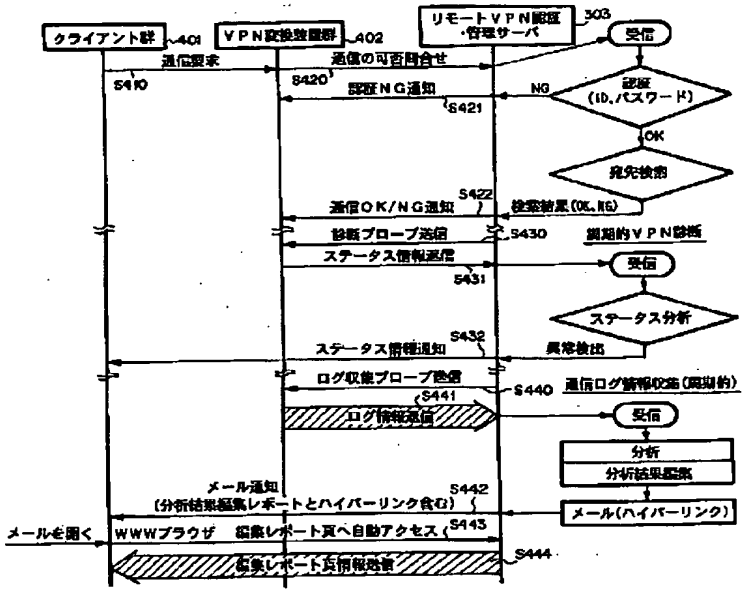
【図２】


リモートＶＰＮ認証・管理サーバ(マスター&スレーブ)機能構成図
－記憶部－
－加入者管理・認証・ＣＡ発行－
クライアント群、ＶＰＮ変換装置群、マスター・サーバ、スレーブ・サーバ群(From TO)
201
加入者情報記憶部
211
ＶＰＮ変換装置認証機能
202
ＶＰＮ変換装置情報記憶部
212
ＣＡ発行・登録機能
203
X.509ディレクトリ記憶部
213
X.509ディレクトリ記憶部検索機能
214
通信制御・制御機能
250
対外部送受信機能
－通信履歴記憶部－
－周期診断、ログ収集、レポート送信－
204
加入者通信履歴記憶部
220
ＶＰＮ変換装置診断分析機能
223
加入者通知機能
205
ＶＰＮ通信履歴記憶部
221
ログ情報収集機能
224
ログ情報分析機能
206
スレーブ通信履歴記憶部(マスター・サーバ)
222
スレーブＤＢレプリケーション機能(マスター・サーバ)
225
分析結果編集機能
226
編集文書送信機能
－システム・リコンフィグレーション－
230
システム・リコンフィグレーション機能
240
スレーブ診断機能(マスター・サーバ)
241
スレーブ診断分析機能(マスター)
242
最適代替スレーブ選択機能(マスター)
245
スレーブ担当情報検索・収集機能(マスター・サーバ)
243
最適スレーブ・リロケーション機能(マスター・サーバ)

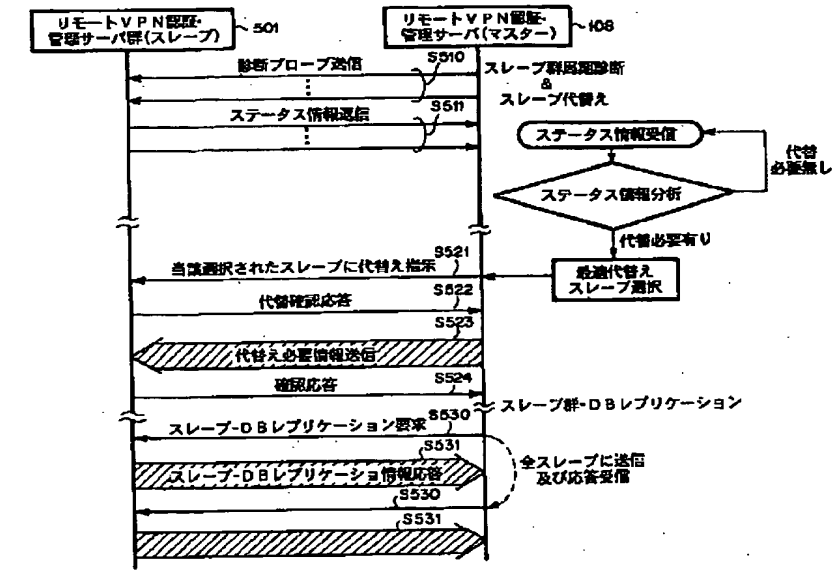
【図３】


リモートＶＰＮ認証・管理サーバとの動作図
クライアント
301
ＶＰＮ変換装置
302
リモートＶＰＮ認証・管理サーバ
303
加入申請書
郵送又は手渡
S301
加入申請書
受付
加入審査
NG
OK
加入登録書
ID番号etc.
郵送又は手渡
S302
メール通知(加入ＮＧ)
S303
認証証発行要求
S310
受信
認証(ID、パスワードetc.)
NG
OK
認証証発行
S311
認証ＮＧの旨返信
S312

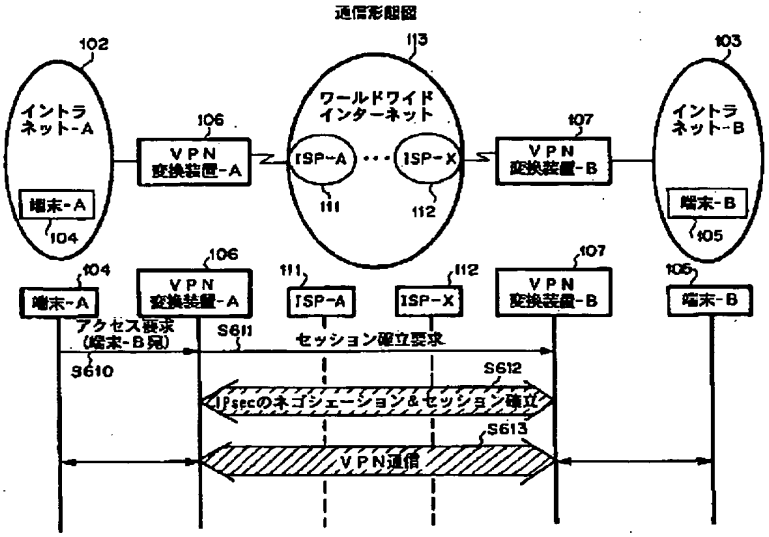
【図４】


クライアント群
401
VPN変換装置群
402
リモートVPN認証・管理サーバ
303
受信
通信要求
S410
通信の可否問合せ
S420
認証NG通知
S421
NG
認証(ID,パスワード)
OK
宛先検索
通信OK/NG通知
S422
検索結果(OK,NG)
診断プローブ送信
S430
周期的VPN診断
ステータス情報送信
S431
受信
ステータス分析
ステータス情報通知
S432
異常検出
ログ収集プローブ送信
S440
通信ログ情報収集(周期的)
S441
ログ情報送信
受信
分析
分析結果蓄積
メール通知
(分析結果蓄積レポートとハイパーリンク含む)
S442
メール(ハイパーリンク)
メールを開く
WWWブラウザ
蓄積レポート頁へ自動アクセス
S443
蓄積レポート頁情報送信
S444

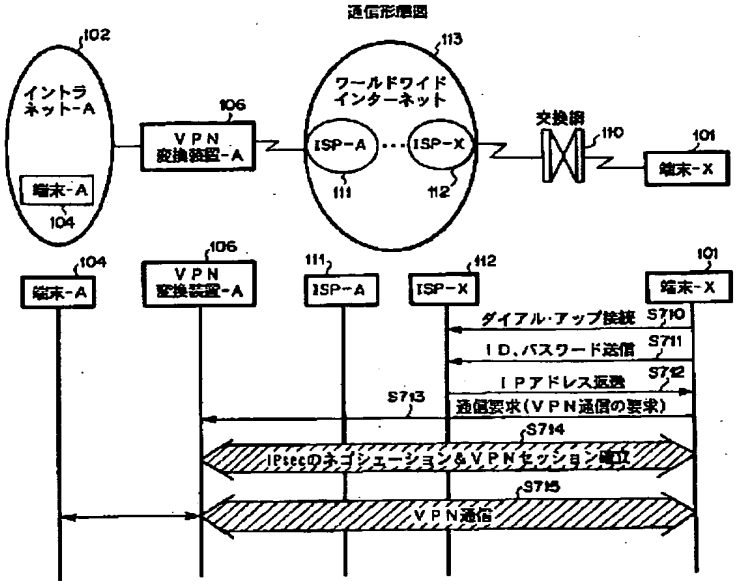
【図５】


リモートVPN認証・管理サーバ群(スレーブ)
501
リモートVPN認証・管理サーバ(マスター)
108
診断プローブ送信
S510
スレーブ群周期診断
&
スレーブ代替え
ステータス情報送信
S511
ステータス情報受信
代替必要無し
ステータス情報分析
代替必要有り
当該選択されたスレーブに代替え指示
S521
最適代替えスレーブ選択
代替確認応答
S522
S523
代替え必要情報送信
確認応答
S524
スレーブ群-DBレプリケーション
スレーブ-DBレプリケーション要求
S530
S531
スレーブ-DBレプリケーション情報応答
全スレーブに送信及び応答受信
S530
S531

【図６】


通信形態図
102
イントラネット-A
端末-A
104
106
VPN変換装置-A
113
ワールドワイドインターネット
ISP-A
ISP-X
111
112
107
VPN変換装置-B
103
イントラネット-B
端末-B
105
アクセス要求(端末-B宛)
S610
S611
セッション確立要求
S612
IPsecのネゴシエーション&セッション確立
S613
VPN通信

【図７】


通信形態図
102
イントラネット-A
端末-A
104
106
VPN変換装置-A
113
ワールドワイドインターネット
ISP-A
ISP-X
111
112
交換網
110
101
端末-X
ダイアル・アップ接続
S710
ＩＤ，パスワード送信
S711
ＩＰアドレス返送
S712
S713
通信要求(ＶＰＮ通信の要求)
S714
IPsecのネゴシエーション&VPNセッション確立
S715
ＶＰＮ通信